

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

In re Morgan Stanley Data Security Litigation

20 Civ. 5914 (AT)

**PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO
MORGAN STANLEY SMITH BARNEY LLC'S MOTION TO DISMISS**

PRELIMINARY STATEMENT	1
STATEMENT OF FACTS	2
STANDARDS OF REVIEW	6
ARGUMENT	7
A. Plaintiffs Satisfy Article III Standing Requirements.....	7
1. This is Not a “Data Loss” Case.....	7
2. Plaintiffs’ Injuries Confer Article III Standing	9
B. Plaintiffs Adequately Allege Both Common Law and Statutory Claims.....	17
1. Plaintiffs Adequately Allege Negligence and Gross Negligence Claims	17
2. Plaintiffs’ New York GBL Claim is Adequate and Timely.....	20
3. Plaintiffs Adequately Allege a Breach of Fiduciary Duty Claim	26
4. Plaintiffs Adequately Allege an Unjust Enrichment Claim	28
5. Plaintiffs Adequately Allege a Breach of Confidence Claim	29
CONCLUSION.....	30

TABLE OF AUTHORITIES

<u>Case</u>	<u>Page</u>
<i>Amidax Trading Grp. V. S.W.I.F.T. SCRL</i> , 671 F.3d 140 (2d Cir. 2011)	10
<i>Andre Strishak & Assocs., P.C. v. Hewlett Packard Co.</i> , 300 A.D. 2d 608 (2002).....	20
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	6
<i>ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.</i> , 493 F.3d 87 (2d Cir. 2007)	6
<i>Baldini v. Shah</i> , 2018 WL 11226079 (S.D.N.Y. Aug 9, 2018)	7
<i>Banco de La Republica de Colombia v. Bank of New York Mellon</i> , 2013 WL 3871419 (S.D.N.Y. July 26, 2013)	22
<i>Bass v. Facebook</i> , 394 F. Supp. 3d 1024 (N.D. Cal. 2019)	14
<i>Beck v. McDonald</i> , 848 F.3d 262 (4th Cir. 2017).....	8
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	6
<i>Boule v. Hutton</i> , 328 F.3d 84 (2d Cir. 2003)	23
<i>Brush v. Miami Beach Healthcare Grp., Ltd.</i> , 238 F. Supp. 3d 1359 (S.D. Fla. 2017).....	18
<i>C.J. by & through Brady v. Truman Med. Ctr., Inc.</i> , 2020 WL 3473651 (W.D. Mo. June 25, 2020)	18
<i>Chambers v. Time Warner, Inc.</i> , 282 F.3d 147 (2d Cir. 2002)	7
<i>Chanko v. Am. Broad. Cos.</i> , 27 N.Y.3d 46 (2016)	29
<i>Chiarelli v. Nissan N. Am., Inc.</i> , 2015 WL 5686507 (E.D.N.Y. Sept. 25, 2015)	25
<i>City of Almaty v. Sater</i> , 503 F. Supp. 3d 51 (S.D.N.Y. 2020)	22
<i>Clapper v. Amnesty International USA et al.</i> , 133 S. Ct. 1138 (2013)	8, 14
<i>Cohen v. Northeast Radiology, P.C.</i> , 2021 WL 293123 (S.D.N.Y. Jan. 28, 2021).....	24
<i>Crupar-Weinmann v. Paris Baguette Am., Inc.</i> , 861 F.3d 76, 79 (2d Cir. 2017)	16
<i>Cummings v. FCA US LLC</i> , 401 F. Supp. 3d 288 (N.D.N.Y. 2019)	16
<i>Daly v. Metro. Life Ins. Co.</i> , 782 N.Y.S.2d 530 (Sup. Ct. 2004).....	27, 29
<i>Democratic Ass'n v. Brandi</i> , 2014 WL 2589279 (D. Conn. June 10, 2014)	14

<i>Deskovic v. City of Peekskill</i> , 673 F. Supp. 2d 154 (S.D.N.Y. 2009).....	19
<i>Dubuisson v. Stonebridge Life Ins. Co.</i> , 887 F.3d 567 (2d Cir. 2018).....	15, 16
<i>E.P. Lehmann Co. v. Polk’s Modelcraft Hobbies, Inc.</i> , 770 F. Supp. 202 (S.D.N.Y. 1991).....	27
<i>EBC I, Inc. v. Goldman, Sachs & Co.</i> , 5 N.Y.3d 11 (2005)	27
<i>Eurycleia Partners, LP v. Seward & Kissel, LLP</i> , 12 N.Y.3d 553 (2009)	27
<i>Fernandez v. Leidos, Inc.</i> , 127 F. Supp. 3d 1078 (E.D. Cal. 2015).....	11
<i>Fero v. Excellus Health Plan, Inc.</i> , 236 F. Supp. 3d 735 (W.D.N.Y. 2017)	12, 24
<i>Fero v. Excellus Health Plan, Inc.</i> , 502 F. Supp. 3d 724 (W.D.N.Y. 2020)	21
<i>Galaria v. Nationwide Mutual Ins. Co.</i> , 663 F. App’x 384 (6th Cir. 2016)	14, 15
<i>General Stencils v. Chiappa</i> , 219 N.E.2d 169 (N.Y. 1966).....	22
<i>Goldenberg v. Johnson & Johnson Consumer Cos.</i> , 8 F. Supp. 3d 467 (S.D.N.Y. 2014)	23
<i>Healthcare Strategies, Inc. v. ING Life Ins. & Annuity Co.</i> , 2012 WL 162361 (D. Conn. Jan. 19, 2012).....	20
<i>Hedges v. Obama</i> , 724 F.3d 170 (2d Cir. 2013).....	14
<i>Hinds Cty., Miss. v. Wachovia Bank N.A.</i> , 700 F. Supp. 2d 378 (S.D.N.Y. 2010).....	18, 19
<i>Hutton v. Nat’l Bd. of Examiners in Optometry, Inc.</i> , 892 F.3d 613 (4th Cir. 2018)	8
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016)	15
<i>In re Anthem, Inc. Data Breach Litig.</i> , 2016 WL 3029783 (N.D. Cal. May 27, 2016).....	16
<i>In re Arby’s Rest. Grp., Inc., Litig.</i> , 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018)	18
<i>In Re Blackbaud, Inc., Customer Data Breach Litigation</i> , 2021 WL 2718439 (D.S.C. July 1, 2021)	9
<i>In re Cap. One Consumer Data Sec. Breach Litig.</i> , 488 F. Supp. 3d 374 (E.D. Va. 2020)	14, 28, 29
<i>In re Equifax, Inc., Customer Data Sec. Breach Litig.</i> , 362 F. Supp. 3d 1295 (N.D. Ga. 2019)	17, 18
<i>In re Equifax Inc. Customer Data Sec. Breach Litig.</i> , 999 F.3d 1247 (11th Cir. 2021)	10, 11
<i>In re GE/CBPS Data Breach Litig.</i> , 2021 WL 3406374 (S.D.N.Y. Aug. 4, 2021)	12

<i>In re: The Home Depot, Inc., Cust. Data Sec. Breach Litig.</i> , 2016 WL 2897520 (N.D. Ga. May 18, 2016)	18
<i>In re JetBlue Airways Corp. Priv. Litig.</i> , 379 F. Supp. 2d 299 (E.D.N.Y. 2005)	28
<i>In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.</i> , 440 F. Supp. 3d 447 (D. Md. 2020)	14, 18
<i>In re Michaels Stores Pin Pad Litig.</i> , 830 F. Supp. 2d 518 (N.D. Ill. 2011)	18
<i>In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.</i> , 45 F. Supp. 3d 14 (D.D.C. 2014)	9, 10
<i>In re Signet Jewelers Limited Securities Litigation</i> , 389 F. Supp. 3d 221 (S.D.N.Y. 2019)	24
<i>In re Target Corp. Cust. Data Sec. Breach. Litig.</i> , 64 F. Supp. 3d 1304 (D. Minn. 2014)	18
<i>In re Yahoo! Inc. Customer Data Breach Litig.</i> , 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)	16
<i>Intellectual Cap. Partner v. Institutional Credit Partners LLC</i> , 2009 WL 1974392 (S.D.N.Y. July 8, 2009)	28
<i>J.S. ex rel. N.S. v. Attica Cent. Sch.</i> , 386 F.3d 107 (2d Cir. 2004)	6
<i>Jones v. Commerce Bancorp, Inc.</i> , 2006 WL 1409492 (S.D.N.Y. May 23, 2006)	27, 30
<i>Kamal v. J. Crew Grp., Inc.</i> , 918 F.3d 102 (3d Cir. 2019)	30
<i>Katz v. Pershing, LLC</i> , 672 F.3d 64 (1st Cir. 2012)	7
<i>Kosakow v. New Rochelle Radiology Assocs., P.C.</i> , 274 F.3d 706 (2d Cir. 2001)	21
<i>Lewert v. P.F. Chang's China Bistro</i> , 819 F.3d 963 (7th Cir. 2016)	14
<i>Lujan v. Defs. of Wildlife</i> , 504 U.S. 555 (1992)	19
<i>Mackey v. Belden, Inc.</i> , 2021 WL 3363174 (E.D. Mo. Aug. 3, 2021)	19
<i>Marshall v. Conway Reg'l Med. Ctr.</i> , 2020 WL 5746839 (E.D. Ark. Sept. 25, 2020)	18
<i>Maurizio v. Goldsmith</i> , 230 F.3d 518 (2d Cir. 2000)	20
<i>McFarlane v. Altice USA, Inc.</i> , 2021 WL 860584 (S.D.N.Y. Mar. 8, 2021)	12
<i>McGhan v. Ebersol</i> , 608 F. Supp. 277 (S.D.N.Y. 1985)	26
<i>McGuire v. Shubert</i> , 722 A.2d 1087 (Pa. Super. Ct. 1998)	29

<i>McMorris v. Carlos Lopez & Associates, LLC</i> , 995 F.3d 295 (2d Cir. 2021).....	7, 9, 10, 12, 13, 15
<i>Morgan Stanley & Co. Inc. v. JP Morgan Chase Bank, N.A.</i> , 645 F. Supp. 2d 248 (S.D.N.Y. 2009).....	17
<i>Nick v. Target Corp.</i> , 2017 WL 10442061 (E.D.N.Y. Sept. 13, 2017)	25
<i>Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank</i> , 85 N.Y.2d 20 (1995)	20, 25
<i>Peterson v. Idaho First Nat. Bank</i> , 367 P.2d 284 (Idaho 1961)	29
<i>Quinn v. Walgreen Co.</i> , 958 F. Supp. 2d 533 (S.D.N.Y. 2013).....	23
<i>Remijas v. Neiman Marcus Group, LLC</i> , 794 F.3d 688 (7th Cir. 2015).....	14, 15
<i>Reilly v. Ceridian Corp.</i> , 664 F.3d 38 (3d Cir. 2011)	7
<i>Reprosystem, B.V. v. SCM Corp.</i> , 727 F.2d 257 (2d Cir. 1984)	28
<i>Rudolph v. Hudson's Bay Co.</i> , 2019 WL 2023713 (S.D.N.Y. May 7, 2019).....	14, 28
<i>Sachs v. Cluett, Peabody & Co.</i> , 39 N.Y.S.2d 853, 856 (1st Dept. 1943).....	26
<i>Sackin v. TransPerfect Glob., Inc.</i> , 278 F. Supp. 3d 739 (S.D.N.Y. 2017)	28
<i>Sims v. First Consumers Nat'l Bank</i> , 758 N.Y.S. 2d 284 (1st Dep't 2003).....	23
<i>Singh v. Cigna Corp.</i> , 918 F.3d 57 (2d Cir. 2019).....	23
<i>Small v Lorillard Tobacco Co.</i> , 94 N.Y. 2d 43 (1999)	20
<i>Spokeo v. Robins</i> , 136 S. Ct. 1540 (2016)	16
<i>St. John's Univ., New York v. Bolton</i> , 757 F. Supp. 2d 144 (E.D.N.Y. 2010)	21
<i>Stagl v. Delta Airlines</i> , 52 F.3d 463 (2d Cir. 1995)	17
<i>TransUnion LLC v. Ramirez</i> , 141 S. Ct. 2190 (2021)	9
<i>U.S. Bank Nat'l Ass'n v. Ables & Hall Builders</i> , 696 F. Supp. 2d 428 (S.D.N.Y. 2010).....	27
<i>Wallace v. Health Quest Sys., Inc.</i> , 2021 WL 1109727 (S.D.N.Y. March 23, 2021)	15, 16, 24, 25
<i>Whitney v. Citibank, N.A.</i> , 782 F.2d 1106 (2d Cir. 1986).....	26
<i>Wilner v. Allstate Ins. Co.</i> , 71 A.D. 3d 155 (2d Dept. 2010).....	26

<i>Woods v. Maytag Co.</i> , 2010 WL 4314313 (E.D.N.Y. 2010)	23
<i>Zorrilla v. Carlson Restaurants Inc.</i> , 255 F. Supp. 3d 465 (S.D.N.Y. 2017)	20, 21
<i>Zumpano v. Quinn</i> , 849 N.E.2d 926 (N.Y. 2006)	22

Federal Rule of Procedure

Page

Fed. R. Civ. P. 12(b)(1).....	6
Fed. R. Civ. P. 12(b)(6).....	6, 12, 20

Statute

Page

New York General Business Law § 349.....	<i>passim</i>
New York General Business Law § 899-aa.....	22, 23

PRELIMINARY STATEMENT

Plaintiffs' Consolidated Amended Class Action Complaint (the "Complaint" or "CAC") describes in exacting detail how Defendant, Morgan Stanley Smith Barney, LLC ("Morgan Stanley"), divulged to unauthorized third parties the personally identifiable and financial information ("PII") of 14.5 million current and former clients (the "2016 Incident"). In an effort to save \$100,000 (roughly 0.0017% of its 2016 revenue), Morgan Stanley dismissed IBM in favor of an unknown and unqualified vendor to decommission its computer equipment. Morgan Stanley maintained its reckless behavior through the decommissioning by, *inter alia*, failing to ensure and verify that its vendors followed proper sanitization and disposal practices, and allowing the equipment to be sold online with unencrypted client PII still intact, with Morgan Stanley keeping the majority of the sale proceeds. When Morgan Stanley was informed by a third party that the used equipment was sold with labels identifying Morgan Stanley as its source, and with client PII in readable form, Morgan Stanley commenced an investigation directed more at concealing evidence of its wrongdoing than searching for the truth. That investigation failed to identify and locate an overwhelming majority of its decommissioned devices. Plaintiffs' counsel has located one such device and can demonstrate that client PII is accessible and readable in plain text.

History repeated itself in 2019 when Morgan Stanley again failed to sanitize its servers before transferring them to a third party and, because it did not follow chain of custody procedures, could not locate those devices containing client PII. Morgan Stanley substantially ignores these and a plethora of additional allegations in its Motion to Dismiss (the "Motion" or "Mot."), instead suggesting that Plaintiffs lack Article III standing to hold Morgan Stanley accountable for its reckless disregard of their privacy. But that contention is entirely unmoored from the low threshold governing Plaintiffs' allegations at this stage, and contrary to ample additional facts Plaintiffs allege in copious detail in the Complaint, all of which compel denial of Morgan Stanley's Motion.

STATEMENT OF FACTS

The 2016 Incident was precipitated by Morgan Stanley’s profit-driven decisions to: (1) terminate a contract with its long-standing vendor IBM for the decommissioning, wiping, and destruction of computer equipment; (2) hire a local moving company with no information technology asset disposal (“ITAD”) experience to do the job; and (3) fail to supervise the project. CAC ¶¶ 1–3. The Morgan Stanley personnel responsible for overseeing the project—including the vice president who was terminated for his role in the events—ignored industry standards, electing instead to save approximately \$100,000 by selecting a non-ITAD vendor for the job, and choosing the “poor man’s wipe” when decommissioning the equipment, which IBM, Morgan Stanley, and others knew would leave unencrypted data intact on the equipment. CAC ¶¶ 46, 47, 52, 83, 87–89, 114–16.

For the decommissioning, Morgan Stanley contracted with Triple Crown, a local moving company, who in turn was using WeedHire (formerly known as AnythingIT) to assist in the disposal and resale of Morgan Stanley’s used devices. CAC ¶¶ 7(h), 34–36. WeedHire/AnythingIT, the company that was ostensibly to sanitize the equipment, was well-known to and approved by Morgan Stanley. CAC ¶¶ 94, 95. WeedHire had shifted its priorities from the data destruction business to acting as a legalized marijuana job bank. Morgan Stanley considered WeedHire to be a “high risk” vendor with which it was not supposed to do business. CAC ¶¶ 7(f), 37. Nevertheless, Morgan Stanley not only used WeedHire for the project, but pressed to make decommissioning assets a “profit center,” attempting to cut costs at every corner. CAC ¶¶ 6, 33.

A year after the completion of the decommissioning project, Morgan Stanley was contacted by a third party, “Mr. Oklahoma,” who had purchased its used equipment on the internet. CAC ¶¶ 7, 18. Mr. Oklahoma contacted Morgan Stanley at an internal private email address in October 2017, writing: “I recently purchased NetApp gear from eBay. [Upon turning it on], *I had access*

to all of your data that was on the equipment sold to us from a third party.” CAC ¶ 7(h) (emphasis added). Morgan Stanley did not immediately ask Mr. Oklahoma to stop using the equipment or arrange to promptly inspect or retrieve the equipment or contact Mr. Oklahoma’s employer, the purchaser of the equipment. CAC ¶ 7(j). Instead, despite knowing that Mr. Oklahoma had unfettered access and control of client PII, Morgan Stanley simply asked him to overwrite the data to destroy any evidence of its disclosure. CAC ¶¶ 7(j)–(k). Morgan Stanley finally retrieved the equipment some months later, but only after, at their direction, Mr. Oklahoma tampered with the devices in an effort to destroy evidence that Morgan Stanley client data had existed on them. CAC ¶ 7(k). Morgan Stanley paid Mr. Oklahoma approximately \$40,000 for his efforts, in addition to certain legal fees, and his consent to a non-disclosure agreement. CAC ¶¶ 7(j)–(k). Thousands of additional pieces of IT equipment containing unencrypted Morgan Stanley client PII that were sold on the internet remain in the hands of other third party purchasers, who have the skills that enable them to access Plaintiffs’ and Class members’ PII. CAC ¶¶ 3, 7, 18, 51, 95, 152.

Morgan Stanley withheld notice of the 2016 Incident for years. CAC ¶ 8. Morgan Stanley only disclosed the Incident to its clients after being compelled to do so by the Office of the Comptroller of Currency (“OCC”). CAC ¶ 9. At that point, some four years after the fact, millions of former Morgan Stanley clients learned that their PII had been exposed. CAC ¶¶ 13, 23, 59–67.

Morgan Stanley’s conduct is contrary to representations that it made to the public, regulators, and its clients. CAC ¶¶ 4, 192–95, 204. On its website,¹ Morgan Stanley represents that safeguarding client assets and personal information is “among [its] highest priorities.” CAC ¶ 204. Despite this proclamation, Morgan Stanley admitted to the New Jersey Attorney General that the

¹ The website is referenced in footnote 23 as part of ¶ 23 of the CAC: ¶¶ 4: <https://www.morganstanley.com/what-we-do/wealth-management/online-security>

drives were not encrypted. CAC ¶¶ 30, 138. Morgan Stanley publicly and unequivocally acknowledges its fiduciary relationship with clients for whom it acts as an investment adviser. CAC ¶ 75. In its “Privacy Pledge” to its clients as of March 17, 2016, Morgan Stanley promised that it would safeguard client PII and assured clients that protecting the confidentiality and security of their information is an integral part of how it conducts its business. CAC ¶¶ 4, 204. In its U.S. Customer Privacy Notice—which it is required by law to disseminate, Morgan Stanley claims it uses security measures that comply with federal law and has policies governing the proper handling of PII by internal personnel as well as third parties. CAC ¶ 5.

The sequence of events that directly precipitated and followed the 2016 Incident reflects a pervasive culture of dereliction, secrecy, and deception among Morgan Stanley personnel charged with protecting its clients’ PII. CAC ¶¶ 2, 7(a), 101. Morgan Stanley had an established decommissioning procedure, but due to its desire for a “quick recovery[,]” Morgan Stanley chose not to follow that procedure. CAC ¶¶ 103–106. As Morgan Stanley internally—and unsuccessfully—tried to account for its decommissioned devices after Mr. Oklahoma’s email, the vice president admitted to his colleagues that Morgan Stanley had used asset inventory control software to track decommissioned devices during early in the project, but then stopped doing so. CAC ¶ 102. As a result, Morgan Stanley had no internal records to verify the disposition of its decommissioned IT Assets. CAC ¶¶ 3, 10, 102, 152.

Morgan Stanley Conceals the Exposure of its Clients’ Data

Some of the devices Morgan Stanley retrieved from Mr. Oklahoma still contained its clients’ PII even upon their return. CAC ¶ 143. Morgan Stanley worked with Stroz Friedberg (“Stroz”), a supposedly independent forensic firm, to exonerate itself as the source of that PII. Stroz solicited comments from Morgan Stanley counsel on its report, both orally and in writing,

over a period of months prior to issuing that report. CAC ¶¶ 55, 148. Of the more than 4,900 known devices that Morgan Stanley contracted with Triple Crown to decommission in 2016, only 246 hard drives were provided to Stroz. CAC ¶¶ 34, 145. These 246 devices were grouped by Morgan Stanley—not Stroz—into tiers based on Morgan Stanley’s internal assessment of the likelihood they contained client PII, and Stroz searched those drives for a list of patterns and keywords provided by Morgan Stanley. CAC ¶¶ 142–48. Stroz found Morgan Stanley’s clients’ Social Security numbers and other PII on the devices, but worked with Morgan Stanley to creatively rule out Morgan Stanley as the source for that PII. CAC ¶¶ 147, 149–151.

Countless internet purchasers still have Morgan Stanley’s decommissioned equipment in their possession. The whereabouts of this equipment remain unknown. CAC ¶¶ 7, 38. Plaintiffs’ counsel, through independent investigation, recovered some of the missing devices from one such purchaser. Plaintiffs’ expert’s analysis of the recovered devices is unequivocal: the PII (including unencrypted Social Security numbers, banking information, addresses, telephone numbers, and account numbers for hundreds of thousands of individuals) is accessible—in fact, the PII of one of the named Plaintiffs is on those drives, alongside the name of his Morgan Stanley financial advisor. CAC ¶ 7.

Incredibly, Morgan Stanley failed to learn its lesson from the 2016 Incident. In 2019, Morgan Stanley failed to sanitize “WAAS servers” before transferring them to a third party. CAC ¶ 157–58. Morgan Stanley again failed to follow proper chain of custody procedures, and thus did not discover until February 2020 that it was unable to account for numerous devices. CAC ¶¶ 159–60. Morgan Stanley admitted to the Arkansas Attorney General that previously deleted, unencrypted data was possibly resident on the devices. CAC ¶ 22.

The OCC Consent Decree

Both the 2016 and 2019 Incidents were foreseeable events. An internal 2015 Technology and Information Risk department report references a “[l]ack of evidence to demonstrate compliance with procedure requirements to wipe/degauss assets prior to disposal/reuse,” and adds that “[r]esponsibility/accountability for key activities related to Data Decommissioning require [sic] additional clarity in Firmwide procedures.” CAC ¶ 27. On October 8, 2020, Morgan Stanley entered into a Consent Order with the OCC concerning the Incidents, pursuant to which the OCC assessed a civil penalty of \$60 million, which was at the time an unprecedented amount, finding that, among other things, Morgan Stanley: failed to assess or address the risks associated with decommissioning; failed to assess the risk of using third party vendors; and failed to maintain an appropriate inventory of customer data. CAC ¶ 15. The OCC further found that Morgan Stanley “failed to exercise adequate due diligence in selecting the third-party vendor engaged by Morgan Stanley and failed to adequately monitor the vendor’s performance.” CAC ¶ 15.

STANDARDS OF REVIEW

In reviewing a Rule 12(b)(1) motion, the Court “must accept as true all material factual allegations in the complaint, but [is] not to draw inferences from the complaint favorable to plaintiffs.” *J.S. ex rel. N.S. v. Attica Cent. Sch.*, 386 F.3d 107, 110 (2d Cir. 2004). To withstand a Rule 12(b)(6) motion, “a complaint must contain sufficient factual matter . . . to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Courts must accept the allegations in the complaint as true and draw all reasonable inferences in favor of the non-movant. *ATSI Commc’ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007). This Court has held that “on a motion to dismiss, the Court may consider only the complaint, documents attached to the complaint, matters of which a court can take judicial notice, or documents that the plaintiff knew about and relied upon.”

Baldini v. Shah, 2018 WL 11226079, at *3 (S.D.N.Y. Aug 9, 2018) (citing *Chambers v. Time Warner, Inc.*, 282 F.3d 147, 153 (2d Cir. 2002)). Morgan Stanley repeatedly and improperly relies on evidence outside the scope of those limits (*see, e.g.*, Mot. at 16, referencing without citation Stroz’s alleged efforts to prepare Morgan Stanley device retrieved by Plaintiffs’ counsel for examination by Plaintiffs’ expert), and the Court should disregard all such references.

ARGUMENT

A. Plaintiffs Satisfy Article III Standing Requirements

Plaintiffs have adequately alleged that they are at a substantially increased risk of identity theft after Morgan Stanley disregarded proper policies and protocols for disposal and decommissioning of its computer equipment containing Plaintiffs’ PII. *See, e.g.*, CAC ¶¶ 279, 290, 300, 312, 324, 333, 343, 353. Such allegations exceed the standards for standing recently set forth by the Second Circuit in *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021).

1. This is Not a “Data Loss” Case

Morgan Stanley’s attack on Plaintiffs’ Article III standing allegations is a misapplication of *McMorris*, suggesting that this case is a “data loss” case. It is not; this litigation is a far cry from “data loss” cases in which an employee sends an errant email, a petty thief steals a laptop, or there is a question as to whether confidential information has “been accessed by any unauthorized person.” Mot. at 10. (citing *Katz v. Pershing, LLC*, 672 F.3d 64, 79 (1st Cir. 2012); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40–44 (3d Cir. 2011)). This case is not the result of a mistake; rather, it is the result of Morgan Stanley’s systemic failure to implement industry-standard practices or internal policies for decommissioning thousands of pieces of computer equipment. *See, e.g.*, CAC ¶¶ 2, 7(a), 78, 85. PII is in the hands of and has been accessed by third parties. CAC ¶¶ 7, 41.

In *McMorris*, an employee accidentally sent an internal email and a file with current and former employees’ PII to approximately 65 other employees. *Id.* at 298. The court noted that the

case was akin to, at best, a “misplaced” data case absent evidence of disclosure to an outside party. *Id.* at 299. Further, because the PII had not escaped the company’s network, any other injury allegations were deemed speculative. *Id.* The facts before this Court bear no resemblance to *McMorris*. *McMorris* likened its facts to those in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), in which the plaintiffs alleged a stolen laptop containing their PII was sufficient to confer Article III standing. *Id.* at 274–75. The *Beck* plaintiffs had conducted “extensive discovery,” yet uncovered no evidence that their PII had been accessed or misused, or that any identity theft or other fraud had occurred. *Id.* at 274. The *Beck* court thus reasoned that any injury fell into the “attenuated chain of possibilities” rejected in *Clapper v. Amnesty Int’l USA et al.*, 133 S. Ct. 1138 (2013), and affirmed dismissal of plaintiffs’ case. *Id.* at 275, 277–78.

The Fourth Circuit’s subsequent holding in *Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018), highlights the differences between *Beck* and this case. The *Hutton* court explained that, while in *Beck* “there was no evidence that [a] thief even stole [a] laptop with the intent to steal private information . . . the [*Hutton*] Plaintiffs allege[d] that their data ha[d] been stolen, accessed, and used in a fraudulent manner.” *Id.* at 622. The fact that the *Hutton* plaintiffs did not allege a thief “targeted” their PII did not preclude the court from finding that plaintiffs had suffered injury-in-fact, because they had alleged that their PII—which they had provided to defendant—was misused. *Id.* at 623.

Plaintiffs’ case is vastly different from *McMorris*, *Beck*, and the other “lost data” cases on which Morgan Stanley relies. Plaintiffs’ counsel’s investigation resulted in the recovery of missing devices from a third-party internet purchaser that contained unencrypted PII, including the Social Security number of thousands of individuals, including at least one named Plaintiff. CAC ¶¶ 7, 41. This Court need not engage with any “attenuated chain of possibilities.” Plaintiffs have

demonstrated that a named Plaintiff's PII, as well as the name and contact information of his financial advisor, was actually divulged. CAC ¶ 7(p). And thousands of additional devices sold over the internet have yet to be recovered. CAC ¶ 7.

2. Plaintiffs' Injuries Confer Article III Standing

a. The *McMorris* Factors Support Plaintiffs' Article III standing

McMorris requires courts to consider, among other things: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." 995 F.3d at 303. Even if the Court were to apply only the factors explicitly referenced in *McMorris*, Plaintiffs would maintain Article III standing.

First, Morgan Stanley exposed the PII of approximately 14.5 million current and former clients. Morgan Stanley cites *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), and *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014), cases in which PII was not divulged or readily accessible to outsiders to support its argument that Plaintiffs do not have standing. Data breach cases at the motion to dismiss stage have already begun to distinguish *Ramirez*. The court in *In Re Blackbaud, Inc., Customer Data Breach Litig.*, 2021 WL 2718439 (D.S.C. July 1, 2021), recently found that *Ramirez* does not impact the court's injury in fact analysis at these early stages of litigation, noting that *Ramirez* relied on evidence adduced at trial. *Id.* at *10, n.15.

Further, Morgan Stanley has identified in discovery at least twenty entities that purchased its unencrypted IT Assets containing client PII, some in foreign countries known to be cybercrime havens. CAC ¶¶ 7(g), 130. Mr. Oklahoma attempted to use the IT Assets he purchased, but instead found himself viewing treasure trove of Morgan Stanley data. CAC ¶ 7(h). At least one named

Plaintiff's PII is accessible on a device Plaintiffs' counsel recovered through independent investigation. CAC ¶¶ 7(p), 133. These allegations alone mark a stark distinction from the facts of *In re Science Applications*, where the court found Plaintiffs failed to allege that a thief who broke into a car and stole the car's GPS system, stereo, and several data tapes, knew what the tapes were, knew how to use them, or ever tried to access their contents. 45 F. Supp. 3d at 25. Moreover, in the course of the 2019 Incident, Morgan Stanley transferred its unwiped servers to a third-party vendor with client data largely intact and accessible. CAC ¶ 158. These servers too are unaccounted for. CAC ¶¶ 3, 11, 175. Plaintiffs' allegations defeat any attempt by Morgan Stanley to suggest the PII was not accessed by third parties. *See McMorris*, 995 F.3d at 298, fn.1 (citing *Amidax Trading Grp. V. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011)).

Second, Plaintiffs allege that portions of the data have been misused. Plaintiff Blythe experienced identity theft. CAC ¶ 283. Plaintiff Jaijee's Social Security number was used to fraudulently obtain her bank routing information. CAC ¶ 316. The Nelson Plaintiffs have experienced credit card fraud. CAC ¶ 263. Plaintiff Shapouri also incurred unauthorized charges to her credit card. CAC ¶ 337. In fact, Morgan Stanley's own internal records disclosed during discovery reflect the misuse of its clients' PII. After receiving notice of the Incidents, clients contacted Morgan Stanley to report various forms of fraud and identity theft. Those reports spanned the entire period following the 2016 Incident and included: the submission of fraudulent tax returns using clients' Social Security numbers; the establishment of fraudulent financial accounts; fraudulent applications for employment benefits; and the successful submission of fraudulent loan applications. CAC ¶¶ 13, 23. Other Class Members have contacted Plaintiffs' counsel with reports of similar identity theft. CAC ¶ 24. The allegations in Plaintiffs' Consolidated Amended Complaint are more than sufficient to confer Article III standing. *See In re Equifax Inc.*

Customer Data Sec. Breach Litig., 999 F.3d 1247 (11th Cir. 2021) (“Given the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data, we have no hesitation in holding that Plaintiffs adequately alleged that they face a ‘material’ and ‘substantial’ risk of identity theft”).

Although Morgan Stanley attempts to litigate at the dismissal stage whether it collects credit card information and whether that information was divulged in the 2016, Plaintiffs have plausibly alleged the contrary, that Morgan Stanley does collect credit card numbers, and has requested that its third-party consultant search for them in recovered drives, CAC ¶¶ 76, 134. Further, Plaintiffs plausibly allege that the credit cards belonging to the Nelson Plaintiffs, as well as Plaintiff Shapouri, were misused, CAC ¶¶ 76, 134, 164, 263, 337, and that the misuse was a result of the 2016 Incident. CAC ¶¶ 261–354.

Morgan Stanley attempts to downplay the misuse of PII and identity theft Plaintiffs alleged, citing *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015). *Fernandez* is unavailing and inapposite, as that plaintiff suffered from a plethora of shortcomings in his complaint. In *Fernandez*, the plaintiff alleged that after a backup tape containing his and others’ PII was taken from an employee’s vehicle, a nefarious actor attempted to open a bank account in his name and log in to his email accounts. *Id.* at 1082, 1086. However, because email addresses were not on the tape, the court found that allegation of injury not fairly traceable to the data breach. *Id.* at 1086. The *Fernandez* court further criticized that plaintiff’s theories of harm (*e.g.*, that his medical records were incomplete as a result of the data breach, that inaccuracies on his credit report disqualified him from a job, and that he received an increase in mail advertisements) were too attenuated because they did not have connections to the data involved in the data breach. *Id.* The *Fernandez* court concluded that, in total with these lacking injury allegations, plaintiff’s delay in

filing his complaint, with no evidence of misuse, the injuries were too speculative to demonstrate that he was at a substantial risk of harm. *Id.* 1088.

Here, Plaintiffs have experienced actual—not attempted—identity theft. The *Fernandez* rationale has no basis here. Instead, courts in this Circuit have uniformly held that allegations similar to Plaintiffs as to traceability are sufficient to survive a Rule 12 motion. *See, e.g., In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *4 n.2 (S.D.N.Y. Aug. 4, 2021); *McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (S.D.N.Y. Mar. 8, 2021); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 758–59 (W.D.N.Y. 2017) (“*Fero I*”).

Third, the sensitivity of the PII involved is undisputed. Morgan Stanley’s Notice of Data Breach lists “account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data.” CAC ¶ 201. Morgan Stanley purports to cast doubt on the accessibility of this information. Mot. at 16. But such contentions have no place in a Rule 12 motion. They are also demonstrably false and ignore Plaintiffs’ allegations that their expert accessed the information in unencrypted form. CAC ¶¶ 7, 41. The Court at this stage must accept the allegations in the Complaint as true, and it remains true that Plaintiffs recovered Morgan Stanley equipment from a third-party purchaser, Plaintiffs’ expert was able to access that equipment, and Plaintiffs’ expert located the PII of a named Plaintiff, adjacent to the name of his Morgan Stanley financial advisor, in plain text without encryption on that equipment.

Finally, as the *McMorris* court iterated, the three enumerated factors:

[A]re by no means the only ones relevant to determining whether plaintiffs have shown an injury in fact based on an increased risk of future identity theft or fraud. After all, determining standing is an inherently fact-specific inquiry that “requires careful judicial examination of a complaint’s allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted.”

995 F.3d at 302–03 (citations omitted). Plaintiffs’ allegations regarding Morgan Stanley’s conduct directly implicate the current and future risk of identity theft and fraud now facing Plaintiffs and Class members. Morgan Stanley’s egregious conduct cannot be overstated: in some instances retaining the PII of former clients for decades after the client terminated his or her relationship with Morgan Stanley, including the Nelson Plaintiffs (who closed their account in 2003), Plaintiff Tillman (who closed her account in 2000), the Gamen Plaintiffs (who closed their accounts in 2001 and 2010), and Plaintiff Mausner (who closed his account in 2010). CAC ¶¶ 59, 60, 63, 65, 66. The retained data included historical PII that does not change over a person’s lifetime and is permanently susceptible to misuse (*e.g.*, Social Security numbers and dates of birth). Instead of encrypting its devices to secure the PII, Morgan Stanley left it in plain text accessible to anyone with access to the computer equipment. CAC ¶¶ 36, 41, 106, 128.

Additionally, when Morgan Stanley undertook the decommissioning, it repeatedly cut corners, opting for the cheaper “poor man’s wipe” instead of the more expensive industry-standard redundant erasure techniques. CAC ¶¶ 46, 47, 52, 83, 87–89, 114–16. Although Morgan Stanley conducted an internal risk assessment a year prior to the decommissioning, in which it criticized its failure to comply with requirements to securely erase data contained on equipment prior to disposal, CAC ¶¶ 27, 78, Morgan Stanley persisted with this inadequate practice, further compounding the severity of the 2016 Incident. The egregiousness continued, with Morgan Stanley selecting to resell, rather than destroy, the decommissioned computer equipment. CAC ¶ 81. The decommissioned equipment was sold to the highest bidder. CAC ¶¶ 51, 95, 152. Morgan Stanley selected resale over disposal because of a favorable profit split where Morgan Stanley would take 75% of the proceeds of all sales, further demonstrating Morgan Stanley’s complete indifference to and disregard for Plaintiffs’ and Class Members’ privacy. CAC ¶ 35.

The *McMorris* factors support Plaintiffs' Article III standing, and the Court should reject Morgan Stanley's attempts to minimize Plaintiffs' well-pled Article III standing allegations.

b. Out-of-pocket expenses and time spent establish Article III standing

Morgan Stanley claims that Plaintiffs cannot establish a heightened risk of identity theft, but its own actions reflect otherwise. Plaintiffs received Morgan Stanley's data breach notices and followed Morgan Stanley's recommendation to spend time and effort reviewing their financial accounts for potential fraud, researching credit monitoring and identity theft insurance options, monitor their credit reports for unauthorized charges, and placing freezes on credit files. CAC ¶¶ 264, 268, 273, 278, 284, 289, 294, 299, 306, 311, 318, 319, 323, 328, 332, 338, 342, 347, 352. "It is unlikely that [the defendant] did so because the risk is so ephemeral that it can safely be disregarded." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688,694 (7th Cir. 2015). Plaintiffs were required to spend time they otherwise would have spent on other pursuits. Lost time has consistently been recognized as sufficient injury in data breach cases. *See, e.g., Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713, at *1 (S.D.N.Y. May 7, 2019); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 425 (E.D. Va. Sep. 18, 2020); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460 (D. Md. 2020); *Bass v. Facebook*, 394 F. Supp. 3d 1024, 1035 (N.D. Cal. 2019). The costs Plaintiffs have incurred and will incur are concrete injuries. *See Democratic Ass'n v. Brandi*, 2014 WL 2589279, at *7 (D. Conn. June 10, 2014) (citing *Clapper*, 133 S. Ct. at 1150 n.5; *Hedges v. Obama*, 724 F.3d 170, 195–96 (2d Cir. 2013)). Circuit courts have held that mitigation expenses following an unauthorized disclosure of PII constitute injuries sufficient to confer standing. *See Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963, 967-68 (7th Cir. 2016) (mitigation expenses, e.g., purchasing credit monitoring, and time and effort monitoring financial statements, qualify as "actual injuries"); *Galaria v. Nationwide Mutual Ins. Co.*, 663 F. App'x 384, 388-89 (6th Cir. 2016) (mitigation expenses, including the

time and money spent monitoring bank statements and credit, are reasonable, concrete injuries). *Remijas*, 794 F.3d at 694 (after being notified that her payment card was at risk, purchase of credit monitoring was a reasonable mitigation expense and a concrete injury).

Moreover, expenditures taken to prevent or mitigate harms caused by others are not only cognizable, but required under common law. “[I]t would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, particularly when [the defendant] recommended taking these steps.” *Galaria*, 663 F. App’x at 388. The PII implicated in the 2016 Incident is permanent and not subject to change (*e.g.*, Social Security numbers) and is likely to be used in a manner with long-term and consequential effects. *Cf. McMorris*, 995 F.3d at 303 (finding out-of-pocket expenses to be insufficient where alleged substantial risk of future identity theft is lacking).

c. Plaintiffs lost the benefit of their bargain with Morgan Stanley

Morgan Stanley committed to protect and secure Plaintiffs’ PII. CAC ¶¶ 4, 5, 204. Inherent in Plaintiffs’ relationship with Morgan Stanley was the expectation that Morgan Stanley would use some of the fees it collected from Plaintiffs to implement appropriate data security practices. Morgan Stanley not only failed to do so, but sought to save money by hiring an unqualified vendor to perform such work, and then selling its used equipment to third parties. CAC ¶¶ 7, 45, 51, 95, 152. These allegations have been upheld as satisfying benefit of the bargain damages by a court in this District. *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *8 (S.D.N.Y. March 23, 2021) (citing *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 996 (N.D. Cal. 2016)).

Morgan Stanley asserts that, specifically with respect to NYGBL § 349 claim, a violation of a statutory provision alone does not necessarily constitute an injury-in-fact for the purposes of Article III standing. The Second Circuit held in *Dubuisson v. Stonebridge Life Ins. Co.*, 887 F.3d 567 (2d Cir. 2018), however, that with respect to NYGBL § 349 in particular, “Plaintiffs have

articulated an injury in fact: the difference in price between what they would have paid for the policies with full information and what they in fact paid.” *Id.* at 575 (citing *Crupar-Weinmann v. Paris Baguette Am., Inc.*, 861 F.3d 76, 79 (2d Cir. 2017)). *See also Cummings v. FCA US LLC*, 401 F. Supp. 3d 288, 303–04 (N.D.N.Y. 2019) (citing *Dubuisson*). Plaintiffs adequately allege “benefit of the bargain” damages as to their NYGBL§ 349 claim, as well as a host of other bases on which statutory standing exists. *See infra* § II.B.2.b.

d. Plaintiffs’ PII suffered a diminution in value

Plaintiffs’ allegations are sufficient to maintain their diminution-in-value theory. Plaintiffs’ PII and that of 14.5 million class members is readily accessible in plain text, and is the type of PII commonly sold on the dark web for \$40 to \$200. CAC ¶ 231; *see In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (because a market exists for PII, and criminals typically trade that PII a number of times, there is a value and it is decreased as a result of a breach; allegations for selling the PII is not necessary). “[T]he law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure.” *Spokeo v. Robins*, 136 S. Ct. 1540, 1549 (2016). The Supreme Court’s recent decision in *Ramirez* reflects as much: “Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, *disclosure of private information*, and intrusion upon seclusion.” *Id.* (emphasis added). *See also Wallace*, 2021 WL 1109727, at *8 (citing *In re Yahoo! Inc. Customer Data Breach Litig.*, 2017 WL 3727318, at *13–14 (N.D. Cal. Aug. 30, 2017)) (allegations concerning third party’s access to, misuse, and sale of PII on the dark web are sufficient to establish diminution in value at dismissal stage).

B. Plaintiffs Adequately Allege Both Common Law and Statutory Claims

1. Plaintiffs Adequately Allege Negligence and Gross Negligence Claims

To establish a *prima facie* case for negligence under New York law, plaintiffs must allege (1) a duty owed by the defendant to plaintiffs; (2) breach of that duty; and (3) injuries proximately caused by the breach. *See Stagl v. Delta Airlines*, 52 F.3d 463, 467 (2d Cir. 1995). “[D]uty, in negligence cases, may be defined as an obligation, to which the law will give recognition and effect, to conform to a particular standard of conduct toward another.” *Morgan Stanley & Co. Inc. v. JP Morgan Chase Bank, N.A.*, 645 F. Supp. 2d 248, 255 (S.D.N.Y. 2009) (citation omitted). As the *Morgan Stanley* court further explained, “voluntary assumption of an action imposes a duty of reasonable care in the performance of that action.” *Id.* “Under New York law, anyone who voluntarily assumes a duty can be held liable for negligence in the performance of that duty.” *Id.* (marks and citation omitted). Whether a breach occurred turns on “whether the resulting injury was a reasonably foreseeable consequence of the defendant’s conduct.” *Id.* at 257 (citation omitted). “[T]he harm must be foreseeable at the moment the action is undertaken....” *Id.*

By requiring its clients to disclose their PII in exchange for financial services, Morgan Stanley recognized and assumed a duty to safeguard that PII. *See, e.g.*, CAC ¶¶ 4, 5, 204 (“longstanding commitment to safeguard the privacy of information our clients entrust to us;” “We pledge to continue to ensure that our global business practices protect your privacy;” “protect your personal information from unauthorized access and use”). Having undertaken that duty, Morgan Stanley was required to act with care. CAC ¶¶ 15–18, 27–29, 203, 207, 249–60, 384–85.

Courts applying these principles have held that companies who fail to exercise ordinary care with respect to their customers’ PII owe a duty of care, particularly when, as here, the risk of harm is foreseeable. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019) (Equifax “owed the Plaintiffs a duty of care to safeguard the personal

information in its custody” that arose “from the allegations that [Equifax] knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures”); *In re Arby’s Rest. Grp., Inc., Litig.*, 2018 WL 2128441, at *3–5 (N.D. Ga. Mar. 5, 2018) (same); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) (same); *In re Target Corp. Cust. Data Sec. Breach. Litig.*, 64 F. Supp. 3d 1304, 1309–10 (D. Minn. 2014) (same); *Brush v. Miami Beach Healthcare Grp., Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) (same). “[T]o hold otherwise would create perverse incentives for businesses who profit off of the use of consumers’ [PII] to turn a blind eye and ignore known security risks.” *Equifax*, 362 F. Supp. 3d at 1325 (citing *In re: The Home Depot, Inc., Cust. Data Sec. Breach Litig.*, 2016 WL 2897520, at *1 (N.D. Ga. May 18, 2016)). Plaintiffs’ partial reliance on duties imposed by Section 5 of the FTC Act is not determinative; courts have repeatedly held that federal and state statutes can be used to “establish evidence of the standards of care required by Defendants,” whether or not those statutes have a private right of action. *Marshall v. Conway Reg’l Med. Ctr.*, 2020 WL 5746839, at *2 (E.D. Ark. Sept. 25, 2020); *C.J. by & through Brady v. Truman Med. Ctr., Inc.*, 2020 WL 3473651, at *3 (W.D. Mo. June 25, 2020); *In re Marriott*, 440 F. Supp. at 481. This Court should equally find Morgan Stanley owed such a duty.

Morgan Stanley argues that Plaintiffs’ allegations are “conclusory” and fail to specifically detail how its security practices deviated from acceptable practices. That is not the case. *See, e.g.* CAC ¶¶ 2, 5–7, 35, 46, 82–88, 159, 161, 170, 181, 182, 194, 224. Moreover, Plaintiffs’ allegations would be sufficient even absent those standards. “[I]t is well-settled that ‘[a]t the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss we ‘presum[e] that general allegations embrace those specific facts that are necessary to support the claim.’” *Hinds Cty., Miss. v. Wachovia Bank N.A.*, 700 F. Supp. 2d 378,

393 (S.D.N.Y. 2010) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). That is especially true “where specific details regarding the injury suffered by an individual plaintiff may not be accessible until after discovery.” *Id.*; *see e.g.*, CAC ¶ 27 (Morgan Stanley admitted it lacked evidence reflecting compliance with wiping/degaussing standards prior to disposal; firmwide deficiencies in accounting for key activities related to data decommissioning).

Thus, in another data breach case, *Mackey v. Belden, Inc.*, the court explained that:

“[a]t the motion to dismiss stage, [plaintiff] cannot be expected to have access to detailed information regarding [defendant’s] cybersecurity practices. . . . If after discovery [plaintiff] is unable to identify specific actions [defendant] should have taken to prevent the Data Breach, [defendant] may renew this argument on a motion for summary judgment.”

2021 WL 3363174, at *6 (E.D. Mo. Aug. 3, 2021). Here, Plaintiffs are not required to allege every detail of Morgan Stanley’s deficient security practices when that knowledge is not fully accessible to Plaintiffs before the completion of discovery. Finally, to the extent Morgan Stanley rehashes its standing argument concerning legally cognizable injury traceable to misuse of PII, those arguments fail on the same basis as its standing arguments.

Morgan Stanley’s reliance on *Deskovic v. City of Peekskill*, 673 F. Supp. 2d 154, 161 (S.D.N.Y. 2009), adds nothing. Plaintiffs have alleged—and Morgan Stanley has not disputed—repeated instances in which Morgan Stanley breached applicable standards of the duty of care it owed Plaintiffs, regardless of the actions of non-parties. CAC ¶¶ 2, 5–7, 35, 46, 82–88, 159, 161, 170, 181, 182, 194, 224. For example, Plaintiffs allege Morgan Stanley not only admitted to multiple breaches of duties it owed to Plaintiffs over the course of the decommissioning process, but also breached duties relating to the delay in notifying Plaintiffs and Class Members of the 2016 and 2019 Incidents. CAC ¶¶ 8, 194.

Finally, to the extent Morgan Stanley rehashes its standing-relating argument that Plaintiffs have not alleged legally cognizable injury traceable to misuse of their PII to challenge the sufficiency of Plaintiffs' allegations in support of their negligence claims on the issues of causation and damages, Mot. at 22–23, those arguments fail on the same basis as its standing arguments.²

2. Plaintiffs' New York GBL Claim is Adequate and Timely

New York General Business Law § 349 “prohibits deceptive business practices.” *Andre Strishak & Assocs., P.C. v. Hewlett Packard Co.*, 300 A.D. 2d 608, 609 (2002). A § 349 claim should identify consumer-oriented misconduct which is deceptive and materially misleading to a reasonable consumer, and which causes damages. *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank*, 85 N.Y.2d 20, 25 (1995); *Small v Lorillard Tobacco Co.*, 94 N.Y. 2d 43, 55 (1999); *Maurizio v. Goldsmith*, 230 F.3d 518, 521 (2d Cir. 2000) (citing *Oswego*). Plaintiffs have alleged a timely, well-pled § 349 claim.

a. Plaintiffs' NYGBL § 349 Claim is Not Precluded by the Statute of Limitations

The statute of limitations defense raised by Morgan Stanley “is an affirmative defense, and therefore generally not appropriate for a motion to dismiss.” *Healthcare Strategies, Inc. v. ING Life Ins. & Annuity Co.*, 2012 WL 162361, at *3 (D. Conn. Jan. 19, 2012). In *Zorrilla v. Carlson Restaurants Inc.*, 255 F. Supp. 3d 465, 479 (S.D.N.Y. 2017), this Court detailed the high standard imposed on defendants to properly assert a statute of limitations defense at the dismissal stage, citing Second Circuit appellate precedent:

The lapse of a limitations period is an affirmative defense that a defendant must plead and prove. At the motion to dismiss stage, it is only appropriate to dismiss a claim on statute of limitations grounds if a complaint clearly shows the claim is out of time. Not only must the facts supporting the defense appear on the face of the complaint, but, as with all Rule 12(b)(6) motions, the motion may be granted only

² Morgan Stanley makes the identical argument with regard to Plaintiffs' claim for breach of confidence, and is, likewise, just as unpersuasive. *See* Mot. at 29.

where it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim that would entitle him to relief.

Zorrilla, 255 F. Supp. 3d at 479 (internal citations and quotations omitted).

Morgan Stanley's reliance on *Fero v. Excellus Health Plan, Inc.* is misplaced as this case does not involve a hacking of Morgan Stanley's data systems, but rather a series of conscious and deliberate decisions by Morgan Stanley to not protect customer data during the decommissioning of assets, and to not inform customers that their data was contained on devices sold to the public. Further, Morgan Stanley's argument that Plaintiffs' claims arose when they opened their accounts fails to account for the fact that Plaintiffs' NYGBL claims are based in part on Morgan Stanley's annual misrepresentations regarding its data privacy and security practices which, under federal law, and specifically the Gramm-Leach-Bliley Act, Morgan Stanley had an obligation to disseminate to its clients. CAC ¶¶ 4, 5, 8, 94, 204. These continued and renewed representations made by Morgan Stanley further bolster Plaintiffs' NYGBL claims. *Cf. Fero v. Excellus Health Plan, Inc.*, 502 F. Supp.3d 724, 736–37, 739 (W.D.N.Y. 2020) (“*Fero II*”) (the only privacy notices given were at the beginning of the customer relationship).

In any event, Morgan Stanley is equitably estopped from asserting the statute of limitations defense, as Morgan Stanley continued to engage in violations of § 349 after the 2016 Incident, including by failing to notify Plaintiffs and Class Members of the 2016 Incident, even though it filed an insurance claim to protect its own interest. CAC ¶¶ 8, 18, 194. Morgan Stanley's continued violations and attempts to conceal its deceitful acts equitably estop Morgan Stanley from asserting the statute of limitations defense.

The Second Circuit held in *Kosakow v. New Rochelle Radiology Assocs., P.C.*, 274 F.3d 706, 725 (2d Cir. 2001), that “[w]hether equitable estoppel applies in a given case is ultimately a question of fact.” *See also St. John's Univ., New York v. Bolton*, 757 F. Supp. 2d 144, 187 (E.D.N.Y.

2010) (same, citing New York state precedent). The New York Court of Appeals reiterated the underpinnings of equitable estoppel, observing:

Our courts have long had the power, both at law and equity, to bar the assertion of the affirmative defense of the Statute of Limitations where it is the defendant's affirmative wrongdoing . . . which produced the long delay between the accrual of the cause of action and the institution of the legal proceeding.

Zumpano v. Quinn, 849 N.E.2d 926, 929 (N.Y. 2006) (quoting *General Stencils v. Chiappa*, 219 N.E.2d 169, 171 (N.Y. 1966)). Under New York law, equitable estoppel applies when, as here, “the defendant conceals from the plaintiff the fact that he has a cause of action.” *City of Almaty v. Sater*, 503 F. Supp. 3d 51, 66 (S.D.N.Y. 2020).

“A plaintiff must either allege...specific acts of ‘deceptive conduct’ or ‘a fiduciary relationship which gave the defendant an obligation to inform him or her of facts underlying the claim.’” *Id.* (quoting *Zumpano*) (citations and alterations omitted). Here, Plaintiffs have alleged both. Morgan Stanley publicly acknowledges its fiduciary relationship with its clients, CAC ¶ 75, which the law confirms. *See Banco de La Republica de Colombia v. Bank of New York Mellon*, 2013 WL 3871419, at *11 (S.D.N.Y. July 26, 2013) (citing New York cases holding that “investment advisors who have substantial discretion over the investment of their clients' funds owe their clients a fiduciary duty”). That relationship required Morgan Stanley to promptly notify victims of the 2016 Incident.

In addition, Morgan Stanley’s “specific acts of deceptive conduct” would serve to preclude its assertion of the statute of limitations defense—in particular, its decision not to promptly disclose the 2016 Incident. CAC ¶¶ 8, 194. New York General Business Law § 899-aa, requires “[a]ny person or business which owns or licenses computerized data which includes private information” to disclose “any breach of the security of the system following discovery or notification of the breach in the security,” including such instances in which private information

is “*acquired by a person without valid authorization.*” *Id.*, § 899-aa(2) (emphasis added). Morgan Stanley represented to the New York Attorney General, and other regulators, in July 2020—nearly three years after it learned of the 2016 Incident—that it had “no reason to believe that there [had] been any unauthorized access to or unauthorized acquisition of computerized data containing personal information.” CAC ¶¶ 186, 195. However, Morgan Stanley’s representations were also contrary to wide-ranging evidence that Morgan Stanley’s client data has been accessible subsequent to the world-wide sale of its used equipment to internet purchasers beginning in 2016. CAC ¶¶ 3, 7, 18, 51, 95, 152.

b. Morgan Stanley’s Statements and Omissions Violate NYGBL § 349

“To make out a prima facie case under section 349, a plaintiff must demonstrate that (1) the defendant’s deceptive acts were directed at consumers, (2) the acts are misleading in a material way, and (3) the plaintiff has been injured as a result.” *Woods v. Maytag Co.*, 2010 WL 4314313, at *14 (E.D.N.Y. 2010). Plaintiff need not show reliance on the misleading act or practice. *See Boule v. Hutton*, 328 F.3d 84, 94 (2d Cir. 2003). Whether a representation or omission is misleading is a question of fact inappropriate for determination on a motion to dismiss. *See Goldenberg v. Johnson & Johnson Consumer Cos.*, 8 F. Supp. 3d 467, 478 (S.D.N.Y. 2014); *see also Quinn v. Walgreen Co.*, 958 F. Supp. 2d 533, 543 (S.D.N.Y. 2013) (citing *Sims v. First Consumers Nat’l Bank*, 758 N.Y.S. 2d 284 (1st Dep’t 2003)).

Morgan Stanley argues that Plaintiffs’ claim fails because it is premised on “non-actionable statements” that are “generalized” and “puffery.” Morgan Stanley relies on *Singh v. Cigna Corp.*, 918 F.3d 57, 63 (2d Cir. 2019), for its contention that “[c]ourts routinely hold that . . . ‘general statements’ about a company’s ‘integrity’ and ‘compliance with ethical norms’ are too vague and aspirational to constitute actionable misstatements” under § 349, and contend that the statements made in its privacy policies amount to such “aspirations.” Mot. at 25. As the court stated in *In re*

Signet Jewelers Ltd. Sec. Litig., 389 F. Supp. 3d 221, 231 (S.D.N.Y. 2019), however, *Singh* did not rule, as Morgan Stanley implies, that all statements in codes of conduct or privacy policies qualify as puffery. Rather, the *Singh* court expressly stated that context bears on materiality. “Defendant[‘s] interpretation of [*Singh*] asks this Court to do the opposite: ignore all context; just look at the statements in a vacuum; do not consider whether they comport (or contradict) the company’s other disclosures and conduct.” *In re Signet*, 389 F. Supp. at 230. Because of the fiduciary role Morgan Stanley undertook and its affirmative data privacy statements, Plaintiffs were entitled to assume, and did assume, that Morgan Stanley would take appropriate measures to keep their PII safe. CAC ¶¶ 4, 5, 204.

Indeed, courts have repeatedly found statements regarding data privacy similar to those disseminated by Morgan Stanley are actionable. Recently, the court in *Wallace* held:

The Notice of Privacy Practices state Health Quest is “committed to protecting medical information,” and would notify its customers of any potential data breach without any unreasonable delay. It is at least plausible that these statements would have led a reasonable consumer to believe Health Quest employed data security measures adequate to safeguard their information, and that Health Quest would promptly notify them of a data breach.

2021 WL 1109727, at *15; *see Cohen v. Northeast Radiology, P.C.*, 2021 WL 293123, at *9 (S.D.N.Y. Jan. 28, 2021) (holding to similar effect that “it is at least plausible that [defendants’] representations in their [Notice of Privacy Practices] concerning data security [] would lead a reasonable consumer to believe that [defendants] were providing more adequate data security than they purportedly were.”) (quoting *Fero I*, 236 F. Supp. 3d at 776).

With this clear directive from courts in this district, it is unfathomable that Morgan Stanley now seeks to argue that its Privacy Policy and other privacy statements are “non-actionable puffery.” Mot. at 25.

Plaintiffs' § 349 claim is also based on Morgan Stanley's efforts to conceal the 2016 Incident and failing to provide timely and adequate notice to Plaintiffs and class members. *See* CAC ¶¶ 8, 117–51, 194. In *Oswego*, the New York Court of Appeals explained how such omissions may serve as the basis for a § 349 claim:

In the case of omissions in particular—the subject of the present case—the statute surely does not require businesses to ascertain consumers' individual needs and guarantee that each consumer has all relevant information specific to its situation. The scenario is quite different, however, where the business alone possesses material information that is relevant to the consumer and fails to provide this information.

85 N.Y.2d at 25; *see Wallace*, 2021 WL 1109727, at *15 (“Plaintiffs plausibly allege defendant failed to fulfill [their] expectations ... by failing to promptly notify them of any data breach.”); *Fero I*, 236 F.Supp.3d at 775 (quoting *Oswego*). The fact that Morgan Stanley maintained a fiduciary duty to those clients makes its violation that much more egregious. *See Chiarelli v. Nissan N. Am., Inc.*, 2015 WL 5686507, at *12 (E.D.N.Y. Sept. 25, 2015) (“[A] business’s failure to disclose to consumers material, relevant information the business alone possesses is actionable under [GBL] § 349 [even] without reference to any special relationship between the consumer and the business.”).

Finally, Morgan Stanley violated § 349 by failing to disclose to former clients that it would maintain their PII well beyond the customer relation period as well as long beyond regulatory compliance. *See* CAC ¶ 197 (citing 17 C.F.R. § 275.204–2(e)(1)). Courts in the Second Circuit have repeatedly held that similar omissions are actionable. The plaintiffs in *Nick v. Target Corp.*, 2017 WL 10442061, (E.D.N.Y. Sept. 13, 2017), alleged that Target represented that it collected PII strictly for purposes related to filling restricted prescriptions, but failed to disclose that it sold that PII to third parties. The court found that “Plaintiffs sufficiently plead that Target’s conduct constituted actionable omissions under GBL § 349.” *Id.* at *4 (citing *Oswego*).

Morgan Stanley’s final argument in support of its motion to dismiss Plaintiffs’ § 349 claim is that Plaintiffs did not plead injury as a result of deception from Morgan Stanley and that Plaintiffs cannot state a claim under § 349 where their alleged injury is the deceptive conduct itself. “[P]roof that ‘a material deceptive act or practice caused actual, although not necessarily pecuniary harm’ is required to impose compensatory damages.” *Wilner v. Allstate Ins. Co.*, 71 A.D. 3d 155, 161-62 (2d Dept. 2010). The specifics of damages suffered by Plaintiffs and the putative class are stated, *supra* § A(2). Moreover, NYGBL § 349 provides for damages for Plaintiffs’ loss of their “benefit of the bargain.” Here, Plaintiffs would have paid less for Defendant’s services, or selected another wealth management firm, had they been aware of Morgan Stanley’s reckless data security practices. CAC ¶¶ 266, 276, 297, 309, 321, 330, 340, 350. They may have likewise done so had Defendant properly disclosed the 2016 Incident promptly, rather than embarking on a multi-year effort to conceal it.

3. Plaintiffs Adequately Allege a Breach of Fiduciary Duty Claim

The elements of a breach of fiduciary duty claim are: 1) a fiduciary duty existed between the parties; 2) defendant breached that duty; and 3) plaintiffs suffered resulting damages. *Whitney v. Citibank, N.A.*, 782 F.2d 1106, 1115 (2d Cir. 1986). Such a relationship exists between parties “where the parties do not deal on equal terms and one trusts and relies on the other.” *McGhan v. Ebersol*, 608 F. Supp. 277, 285 (S.D.N.Y. 1985) (quoting *Sachs v. Cluett, Peabody & Co.*, 39 N.Y.S.2d 853, 856 (1st Dept. 1943), *aff’d*, 291 N.Y. 772, 53 N.E. 2d 241 (1944)).

Morgan Stanley contends that no fiduciary relationship exists in direct contradiction to its own admissions and documents. Morgan Stanley has publicly and directly acknowledged its fiduciary relationship with clients for whom it acts as an investment adviser. CAC ¶ 75. Plaintiffs and Class Members entrusted sensitive personal and financial information to Morgan Stanley. In

its Privacy Pledge, Morgan Stanley promised to securely protect that PII from disclosure to third parties. CAC ¶¶ 4, 5, 204.

New York courts have recognized the existence of a fiduciary duty in similar contexts. *See Daly v. Metro. Life Ins. Co.*, 782 N.Y.S.2d 530, 535–36 (Sup. Ct. 2004). In *Daly*, after recognizing the existence of a fiduciary relationship for patient PII disclosed in a data breach, the court opined:

Indeed, it is well established under New York law that “a fiduciary duty arises, even in a commercial transaction, where one party reposed trust and confidence in another who exercises discretionary functions for the party’s benefit or possesses superior expertise on which the party relied”. *While this concept has never before been applied to issues surrounding the protection of confidential personal information, perhaps in the absence of appropriate legislative action, it should.*

Id. at 535 (emphasis added) (citations omitted). *See also Jones v. Commerce Bancorp, Inc.*, 2006 WL 1409492, at *3 (S.D.N.Y. May 23, 2006) (citing *Daly* with respect to bank’s disclosure of customer PII).

Importantly, a breach of fiduciary claim is a fact-specific inquiry. *Eurycleia Partners, LP v. Seward & Kissel, LLP*, 12 N.Y.3d 553, 561 (2009); *EBC I, Inc. v. Goldman, Sachs & Co.*, 5 N.Y.3d 11, 19 (2005); *E.P. Lehmann Co. v. Polk’s Modelcraft Hobbies, Inc.*, 770 F. Supp. 202, 205 (S.D.N.Y. 1991). In the single case cited by Morgan Stanley for the premise that there is no general fiduciary duty to secure customer data in New York, *U.S. Bank Nat’l Ass’n v. Ables & Hall Builders*, 696 F. Supp. 2d 428, 442 (S.D.N.Y. 2010), the breach of fiduciary duty claim was dismissed on a motion for summary judgment, after the evidence failed to show plaintiffs placed such a degree of confidence in defendant. Plaintiffs here have adequately alleged that they trusted Morgan Stanley to keep their PII safe and that Morgan Stanley undertook certain responsibilities based on the trust reposed in it by its customers. To the extent it remains to be determined whether such a relationship existed, that is a factual question to be determined at a later stage of the case.

4. Plaintiffs Adequately Allege an Unjust Enrichment Claim

A party should not be allowed to unjustly enrich himself at the expense of another. *Reprosystem, B.V. v. SCM Corp.*, 727 F.2d 257, 263 (2d Cir. 1984). To state a claim for unjust enrichment, a plaintiff must allege that: (1) the defendant was enriched; (2) the enrichment was at plaintiff's expense; and (3) the circumstances were such that equity and good conscience require defendant to make restitution. *Intellectual Cap. Partner v. Institutional Credit Partners LLC*, 2009 WL 1974392, at *8 (S.D.N.Y. July 8, 2009) (applying New York law).

Morgan Stanley's arguments against Plaintiffs' unjust enrichment claim are unpersuasive. Mot. at 27–28. First, the claim is pled in the alternative, and not duplicative. *See* CAC ¶ 456; *see also* Fed. R. Civ. P. 8(a)(3), 8(d)(3). Second, Morgan Stanley's unsupported contention that Plaintiffs "have failed to allege that Morgan Stanley engaged in any inequitable conduct accruing to its benefit," Mot. at 27, is contrary to the facts alleged, and cases upholding unjust enrichment claims based on data disclosure incidents. As the court observed in *Rudolph v. Hudson's Bay Co.*:

Courts have concluded that the failure to secure a plaintiff's data can give rise to an unjust enrichment claim. They reason that a defendant has accepted the benefits accompanying plaintiff's data, but does so at the plaintiff's expense by not implementing adequate safeguards, thus making it "inequitable and unconscionable" to permit defendant to retain funds that it saved by "shirking data-security" and leaving the plaintiff "to suffer the consequences."

2019 WL 2023713, at *12; *see Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017) (denying dismissal of unjust enrichment claim); *In re Cap. One*, 488 F. Supp. 3d at 412 (failure to secure a party's data can give rise to an unjust enrichment claim).

Finally, Morgan Stanley's retention of its former clients' data for years beyond the period required by any law belies its claim that Plaintiffs' data has no value. *Cf. In re JetBlue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 330 (E.D.N.Y. 2005) (dismissing claims where JetBlue shared customer data to prevent future attacks in the wake of September 11, 2001). Indeed,

collecting, maintaining, and protecting PII is vital to many of Morgan Stanley's business purposes. CAC ¶¶ 76, 228. Yet, as data security became a heightened concern for all financial institutions, and others were expanding their efforts to safeguard their clients' PII, Morgan Stanley in 2016 slashed its information technology security budget by 30 percent, chose vendors based strictly on price rather than expertise, and resold its used IT Assets to profit from their decommissioning. CAC ¶ 6. Thus, despite knowing it had had an obligation to protect its customer's PII, it failed to do so, thus making it unjust for it to retain the profits and money it saved by failing to do so.

5. Plaintiffs Adequately Allege a Breach of Confidence Claim

Morgan Stanley contends that Plaintiffs' breach of confidence claim is lacking because New York "does not recognize such a cause of action[.]" Mot. at 28. Morgan Stanley is mistaken. To prevail, a plaintiff must plead: 1) defendant assumed a duty of confidentiality; 2) defendant intentionally, knowingly, or negligently breached that duty; and 3) plaintiff was damaged as a result. *See Chanko v. Am. Broad. Cos.*, 27 N.Y.3d 46, 53–54 (2016). New York courts have sustained such a claim based on a "fail[ure] to safeguard . . . clients' personal and confidential information." *See Daly*, 782 N.Y.S.2d at 535.

The claim has been recognized by other courts to apply particularly against financial institutions for disclosing customer information. *See, e.g., McGuire v. Shubert*, 722 A.2d 1087, 1091 (Pa. Super. Ct. 1998) (recognizing duty between banker and customer that "banker will not divulge to third persons, without the consent of the customer . . . any information relating to the customer acquired through the keeping of his account") (quoting *Peterson v. Idaho First Nat. Bank*, 367 P.2d 284, 290 (Idaho 1961)); *see also, In re Cap. One*, 488 F. Supp. 3d at 409–10 (allowing claims for breach of confidence under Florida and California law because the exposure of financial institution's customer data "was predicated on, at the least, a negligent act on the part of the

Defendants.”). The harm underlying a breach of confidence action “transpires when a third party gains unauthorized access to a plaintiff’s personal information.” *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019).

Moreover, in *Wallace*, the court rejected the defendant’s argument that a duty of confidentiality only exists in the context of communications protected by privilege, such as those between physician-patient. Instead, the *Wallace* court found that a “cloak of confidentiality” extended to a medical corporation that collected PII as a prerequisite for receiving medical services. The *Wallace* court cited *Jones*, 2006 WL 1409492, at *3, where the court found a duty of confidentiality where defendant required plaintiff to disclose personal information and represented that it would safeguard that information. This Court should, too, find that a cloak of confidentiality extends to Morgan Stanley, a corporation that collected customer PII as a prerequisite for confidential and private services and promised to keep that PII safe.

CONCLUSION

For all of the reasons above, Morgan Stanley’s Motion to Dismiss should be denied. Plaintiffs respectfully request leave to replead if the Court grants any portion of the Motion.

Date: September 15, 2021

NUSSBAUM LAW GROUP, P.C.

By: /s/ Linda P. Nussbaum
 Linda P. Nussbaum
 Bart D. Cohen
 Marc E. Foto
 1211 Avenue of the Americas, 40th Fl.
 New York, NY 10036
 (917) 438-9189
 lnussbaum@nussbaumpc.com
 bcohen@nussbaumpc.com
 mfoto@nussbaumpc.com

Respectfully submitted,

MORGAN & MORGAN

By: /s/ Jean S. Martin
 Jean S. Martin
 Ryan J. McGee
 Francesca Kester
 201 N. Franklin Street, 7th Floor
 Tampa, Florida 33602
 (813) 223-5505
 jmartin@ForThePeople.com
 rmcgee@ForThePeople.com
 fkester@ForThePeople.com

Interim Co-Lead Counsel for Plaintiffs